

**CLAIMS**

1. Device for authenticating the taking of pictures made up of digital data comprising a picture taking apparatus and a security element carrying out the signing of at least part of the digital data, characterized in that the security element is a detachable element comprising a decryption circuit with secret key K1, this element being connected to the picture taking apparatus by an interface circuit provided in the picture taking apparatus.
- 5 2. Device according to Claim 1, characterized in that the detachable element incorporates a hashing circuit.

10 150 3. Device according to either of Claims 1 and 2, characterized in that the detachable element is a chip card.

15 a 4. Device according to Claims 1 and 3, characterized in that the picture taking apparatus (1) moreover comprises a multiplexing circuit (6) and a circuit (5) for hashing at least one first fraction (F1 (VN)) of the digital data in such a way as to generate a first hashed datum (m1), the decryption circuit with secret key K1 of the chip card (2) carrying out the decryption of the first hashed datum (m1) in such a way as to generate a signature ( $D(m1)_{K1}$ ) of the first hashed datum (m1), the signature ( $D(m1)_{K1}$ ) and the digital data (VN) being transmitted to the multiplexing circuit (6) so as to constitute a multiplexed signal (S1).

20 30 5. Device according to Claims 2 and 3, characterized in that the picture taking apparatus (1) furthermore comprises a multiplexing circuit (6), a hashing circuit of the chip card carrying out the hashing of at least a first fraction (F1(VN)) of the digital data originating from the picture taking apparatus (8) in such a way as to generate a first hashed datum (m1) and the first hashed datum (m1) is decrypted in the decryption circuit in such a way as to generate a signature ( $D(m1)_{K1}$ ) of the first hashed datum

(m1), the signature ( $D(m1)_{K1}$ ) emanating from the chip card and the digital data (VN) being transmitted to the multiplexing circuit (6) in such a way as to constitute a multiplexed signal (S1).

Claim 1

5. Device according to Claims 1 to 5, characterized in that the picture taking apparatus (1, 8) is a camera head.

Claim 1

6. Device according to Claims 1 to 5, characterized in that the picture taking apparatus (1, 8) is a photographic apparatus.

7. Device for authenticating digital data emanating from a device according to any one of Claim 1, characterized in that it comprises a demultiplexer (11) for separating the digital data (VN)

15 and the signature ( $D(m1)_{K1}$ ), an encryption circuit with public key  $K2$  for calculating an encrypted datum ( $C(D(m1)_{K1})_{K2}$ ) on the basis of the signature ( $D(m1)_{K1}$ ), a circuit (13) for hashing at least one second fraction ( $F2(VN)$ ) of the digital data (VN) emanating from the

20 demultiplexer (11) in such a way as to generate a second hashed datum (m2), a comparison circuit (14) for comparing the encrypted datum ( $C(D(m1)_{K1})_{K2}$ ) with the second hashed datum (m2) in such a way as to constitute a signal (S3) making it possible to verify the

25 authenticity of the digital data.

Rdc  
vo